

INDEMNIFICATION AND DATA SECURITY PROVISIONS

Indemnification Provision

Indemnification

Service Provider shall indemnify, hold harmless, protect and defend Rice and its trustees, officers, employees and representatives (the "Indemnified Parties") for, from and against any and all demands, claims, suits, damages, losses, liabilities, costs and expenses, including, but not limited to, court costs and attorneys' fees (the "Indemnified Matters"), of any nature whatsoever (including, but not limited to, damage to or loss of property, bodily injury or death), directly or indirectly arising out of or in connection with the performance of Service Provider's obligations under this Agreement. Service Provider's indemnification obligations under this Section [] shall apply whether the Indemnified Matters are due in part to the concurrent fault or negligence of the Indemnified Parties or others, but shall not extend to such concurrent fault or negligence. Consultant's defense obligations under this Section [] shall be with attorneys approved by Rice, which approval shall not be unreasonably withheld.

Data Security Provisions

Standard of Care

(a) Service Provider acknowledges and agrees that, in the course of its engagement by Rice, Service Provider may receive or have access to Personal Information. Service Provider shall comply with the terms and conditions set forth in this Agreement in its collection, receipt, transmission, storage, disposal, use and disclosure of such Personal Information and be responsible for the unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of Personal Information under its control or in its possession by all Authorized Employees.

(b) In recognition of the foregoing, Service Provider agrees and covenants that it shall: (i) keep and maintain all Personal Information in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use or disclosure; (ii) use and disclose Personal Information solely and exclusively for the purposes for which the Personal Information, or access to it, is provided pursuant to the terms and conditions of this Agreement, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Personal Information for Service Provider's own purposes or for the benefit of anyone other than Rice, in each case, without Rice's prior written consent; and (iii) not, directly or indirectly, disclose Personal Information to any person other than its Authorized Employees, including any, subcontractors, agents, or auditors (an "Unauthorized Third Party"), without express written consent from Rice unless and to the extent expressly required, by applicable law, in which case, Service Provider shall (i) notify Rice before such disclosure or as soon thereafter as reasonably possible; (ii) be responsible for and remain liable to Rice for the

actions and omissions of such Unauthorized Third Party concerning the treatment of such Personal Information as if they were Service Provider's own actions and omissions; and (iii) require the Unauthorized Third Party that has access to Personal Information to execute a written agreement agreeing to comply with the terms and conditions of this Agreement relating to the treatment of Personal Information.

Confidential Information

For the avoidance of doubt, Service Provider shall treat all information disclosed by Rice pursuant to this Agreement, including Personal Information, as confidential ("Confidential Information"), and Service Provider shall not disclose or use any such Confidential Information except as required in connection with the performance of its obligations under this Agreement as set forth herein.

Information Security

(a) Service Provider represents and warrants that its collection, access, use, storage, disposal and disclosure of Personal Information does and will comply with all applicable federal and, state privacy and data protection laws, as well as all other applicable regulations and directives.

(b) Without limiting Service Provider's obligations under Section [_(a)], Service Provider shall implement administrative, physical and technical safeguards to protect Personal Information that are no less rigorous than accepted industry practices, and shall ensure that all such safeguards, including the manner in which Personal Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Agreement.

Security Breach Procedures

(a) Service Provider shall notify Rice of a Security Breach as soon as practicable, but no later than twenty-four (24) hours after Service Provider becomes aware of it.

(b) Immediately following Service Provider's notification to Rice of a Security Breach, the parties shall coordinate with each other to investigate the Security Breach in accordance with Service Provider's standard policies and procedures, a copy of which [has been provided to Rice/is attached as Exhibit [EXHIBIT NUMBER] to this Agreement.]

(c) Service Provider shall use best efforts to immediately remedy any Security Breach and prevent any further Security Breach at Service Provider's expense in accordance with applicable privacy rights, laws, regulations and standards. Service Provider shall reimburse Rice for actual costs incurred by Rice in responding to, and mitigating damages caused by, any Security Breach, including all costs of notice and/or remediation.

Oversight of Security Compliance

At least once per year, Service Provider shall conduct site audits of the information

technology and information security controls for all facilities used in complying with its obligations under this Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on the recognized industry best practices. Upon Rice's written request, Service Provider shall make available to Rice for review such audit reports. Any exceptions noted on the audit reports will be promptly addressed with the development and implementation of a corrective action plan by Service Provider's management.

Return or Destruction of Confidential Information

At any time during the term of this Agreement at Rice's written request or upon the termination or expiration of this Agreement for any reason, Service Provider shall promptly return to Rice all copies, whether in written, electronic or other form or media, of Rice's Confidential Information in its possession, or securely dispose of all such copies, and certify in writing to Rice that such Confidential Information has been returned to Rice or disposed of securely. Service Provider shall comply with all reasonable directions provided by Rice with respect to the return or disposal of Confidential Information.

Defined Terms

"Authorized Employees" means Service Provider's employees who have a need to know or otherwise access Personal Information to enable Service Provider to perform its obligations under this Agreement.

"Personal Information" means information provided to Service Provider by Rice, or to which access was provided to Service Provider by Rice, in the course of Service Provider's performance under this Agreement that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, financial account numbers, credit report information and other personal identifiers),

"Security Breach" means any act or omission that compromises either the security, confidentiality or integrity of Personal Information or the physical, technical, administrative or organizational safeguards put in place by Service Provider (or any of its contractors or consultants permitted under this Agreement) that relate to the protection of the security, confidentiality or integrity of Personal Information.